PATENT ABSTRACTS OF JAPAN

(11)Publication number : **07-044330**
(43)Date of publication of application : **14.02.1995**

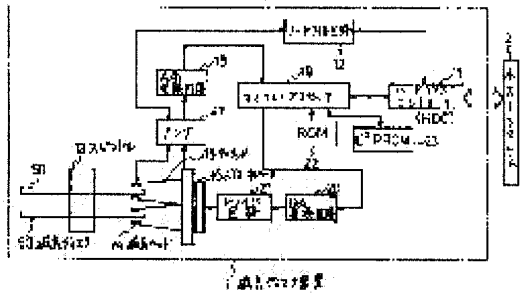
(51)Int.Cl. **G06F 3/06**
G11B 19/02

(21)Application number : **05-186529**
(22)Date of filing : **29.07.1993**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **IGARI CHIKASHI**

(54) MAGNETIC DISK DEVICE AND SURREPTITIOUS USE PREVENTING METHOD FOR RECORDED DATA

(57)Abstract:
PURPOSE: To provide a magnetic disk device and a surreptitious use preventing method for recorded data to prevent the robbery of the recorded data by preventing an easy access carried out by a connected host system.
CONSTITUTION: A microprocessor 19 writes the password sent from a host system 2 into an E2PROM 23 and sets it there. Thereafter no access command is carried out to a magnetic disk 50 from the system 2 as long as a password equal to that received from the system 2 and set at the E2PROM 23 is not supplied when a power supply is switched on. Thus the surreptitious use can be prevented for the recorded data of the disk 50.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－44330

(43)公開日　平成７年(1995)２月14日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　3/06	３０４　Ｈ			
Ｇ１１Ｂ　19/02	５０１　Ｋ	7525－5D		

審査請求　未請求　請求項の数２　ＯＬ　（全　６　頁）

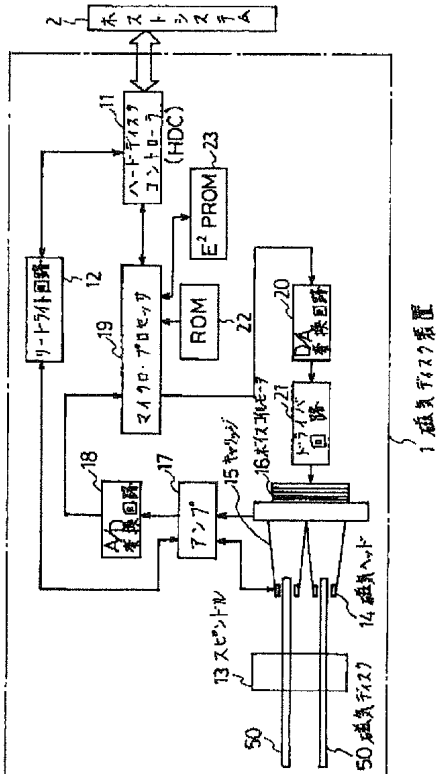
(21)出願番号　特願平5－186529

(22)出願日　平成５年(1993)７月29日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　猪狩　史
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　弁理士　則近　憲佑

(54)【発明の名称】　磁気ディスク装置及び記録データ盗用防止方法

(57)【要約】
【目的】　本発明は、接続したホストシステムからのアクセスを簡単に行えないようにして、記録データの盗難を防止することができる磁気ディスク装置及び記録データ盗用防止方法を提供することを目的としている。
【構成】　本発明において、マイクロプロセッサ１９はホストシステム２から送られてくるパスワードをE^2 ＰＲＯＭ２３に書き込んで設定する。その後、電源オン時に、ホストシステム２からE^2 ＰＲＯＭ２３に設定した前記パスワードと同一のパスワードが入力されない限り、ホストシステム２からの磁気ディスク５０に対するアクセスコマンドを実行しないため、磁気ディスク５０の記録データの盗用が防止される。



1

【特許請求の範囲】

【請求項１】　接続されたホストシステムからのアクセスコマンドにより磁気ディスクに対してデータの読み書きを行う磁気ディスク装置において、書き込み可能な不揮発性メモリと、前記ホストシステムから入力される識別情報を前記不揮発性メモリに記憶して設定する設定手段と、電源起動時、前記不揮発性メモリに設定された識別情報と同一の識別情報が前記ホストシステムから入力されない限り、前記ホストシステムから入力される前記磁気ディスクに対するアクセスコマンドを実行しない制御を行う制御手段とを具備したことを特徴とする磁気ディスク装置。

【請求項２】　接続されたホストシステムからのアクセスコマンドにより磁気ディスクに対してデータの読み書きを行う磁気ディスク装置の前記磁気ディスクに記録されているデータの盗用防止方法にあって、前記ホストシステムから入力される識別情報を設定した後の電源オン時には、設定された前記識別情報と同一の識別情報が前記ホストシステムから入力されない限り、前記ホストシステムから入力される前記磁気ディスクへのアクセスコマンドを実行しないことを特徴とする記録データ盗用防止方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は磁気ディスク装置に係り、特に記録されたデータの盗難を防止する方法に関する。

【０００２】

【従来の技術】近年、磁気ディスク装置はパーソナルコンピュータを始めとする様々な情報処理システムで使用されている。磁気ディスク装置とホストシステムとの接続方法としては、磁気ディスク装置をホストシステムの本体に内蔵する方式、磁気ディスク装置を接続ケーブルを用いてホストシステムに接続する方式が一般的である。ところで、ＰＣＭＣＩＡインタフェース等の規格では、ノートブック型パーソナルコンピュータ等にカードスロットと呼ばれる部分を設け、この部分に磁気ディスク装置等の外部周辺機器を差し込んで使用するという用途が現れている。

【０００３】このようなＰＣＭＣＩＡインタフェースを持つ磁気ディスク装置は、ホストシステムのスロットに直接差し込んで使用することができるので、ホストシステムへの着脱が自在且つ簡単である。しかし、ＰＣＭＣＩＡインタフェースの規格に準拠するような磁気ディスク装置の磁気記録媒体の径は１．８インチ以下が一般的で、大きさも小型化しているために、従来のホストシステムへの組み込み方式やケーブルを用いた接続方式よりも、容易に盗難にあうことが予想される。このような小型磁気ディスク装置の盗難に対する対策としては、ホストシステムがパスワード（識別情報）を記憶しており

2

電源が投入された直後に利用者から正しいパスワードが入力されなければ動作を行わないといった方法がある。しかし、この方法では、利用者が前記パスワードを知っていてさえすれば、接続された磁気ディスク装置が何であれ、その記録データを読み出すことができ、磁気ディスク装置の記録データの盗用防止には有効でないことが分かる。これは、従来の磁気ディスク装置はあくまで据置を前提として作られたものであるため、一旦ホストシステムに接続されれば記憶されている情報に対してのアクセスを妨げる方法が磁気ディスク装置自体には存在していないためで、記録データが盗用されてしまうというような恐れがあった。

【０００４】

【発明が解決しようとする課題】ＰＣＭＣＩＡインタフェースを持つ小型の磁気ディスク装置はホストシステムへの着脱が簡単且つ自在であるため、容易に盗難に遭うことが予想されている。盗難に遭った磁気ディスク装置は同様のホストシステムに接続されれば記録しているデータに対してのアクセスを妨げる方法が磁気ディスク装置自体には存在しないため、記録データが容易に盗用されてしまうという危険性があった。

【０００５】そこで本発明は上記の欠点を除去し、接続したホストシステムからのアクセスを簡単に行えないようにして、記録データの盗用を防止することができる磁気ディスク装置及び記録データ盗用防止方法を提供することを目的としている。

【０００６】

【課題を解決するための手段】本発明は接続されたホストシステムからのアクセスコマンドにより磁気ディスクに対してデータの読み書きを行う磁気ディスク装置において、書き込み可能な不揮発性メモリと、前記ホストシステムから入力される識別情報を前記不揮発性メモリに記憶して設定する設定手段と、電源起動時、前記不揮発性メモリに設定された識別情報と同一の識別情報が前記ホストシステムから入力されない限り、前記ホストシステムから入力される前記磁気ディスクに対するアクセスコマンドを実行しない制御を行う制御手段とを具備した構成を有する。

【０００７】

【作用】本発明の磁気ディスク装置において、設定手段はホストシステムから入力される識別情報を書き込み可能な不揮発性メモリに記憶して設定する。制御手段は電源起動時、前記不揮発性メモリに設定された識別情報と同一の識別情報が前記ホストシステムから入力されない限り、前記ホストシステムから入力される前記磁気ディスクに対するアクセスコマンドを実行しない制御を行う。これにより、磁気ディスク装置が盗まれて別のホストシステムに接続されても、このホストシステムを使用する利用者が前記識別情報を知らない限り、この磁気ディ

データの盗用を防止することができる。

【０００８】

【実施例】以下、本発明の一実施例を図面を参照して説明する。図１は本発明の磁気ディスク装置の一実施例を示したブロック図である。１は磁気ディスク装置、２は前記磁気ディスク装置をＰＣＭＣＩＡインタフェースを介して着脱自在に接続するホストシステムである。磁気ディスク装置１はデータの読み書き制御などを行うハードディスクコントローラ１１、磁気ヘッド１４に対してデータをリードライトするリードライト回路１２、磁気ディスク５０を回転させるスピンドル１３、磁気ディスク５０にデータを読み書きする磁気ヘッド１４、磁気ディスク５０の半径方向に磁気ヘッド１４を移動させるキャリッジ１５、キャリッジ１５を駆動するボイスコイルモータ１６、磁気ヘッド１４で読み出されたサーボデータを増幅するアンプ１７、サーボデータをデジタルデータに変換するＡ／Ｄ変換回路１８、装置全体の制御及び磁気ヘッド１４のシーク制御などを行うマイクロプロセッサ１９、サーボデータをアナログデータに変換するＤ／Ａ変換器１９、ボイスコイルモータ１６を駆動するドライバ回路２１、マイクロプロセッサ１８を制御する各種プログラムや各種データを格納しているＲＯＭ２２、パスワードなどを記憶する書き込み可能な不揮発性メモリであるE^2 ＰＲＯＭ２３を有している。

【０００９】次に本実施例の動作について説明する。図１に示した磁気ディスク装置１を初めて使用する場合など、この装置内にパスワードが設定されていない場合には、利用者はこの磁気ディスク装置１をホストシステム２に装着した後、上記したパスワード情報を設定する操作をホストシステム２のキーボード等から行う。これにより、ホストシステム２はパスワード設定コマンドを磁気ディスク装置１に送る。磁気ディスク装置１のマイクロプロセッサ１９はパスワード設定コマンドをハードディスクコントローラ１１を介して受け取ると、パスワードの転送待ちとなる。一方、利用者はホストシステム２に図３に示したようなパスワードを入力して、このパスワードをハードディスクコントローラ１１を介してマイクロプロセッサ１９に転送させる。マイクロプロセッサ１９はパスワードが転送されてくると、このパスワードをE^2 ＰＲＯＭ２３に書き込んだ後、パスワードが設定されている状態であることを示す情報を同E^2 ＰＲＯＭ２３上に書き込んで処理を終了する。これにより、磁気ディスク装置１内にパスワードが設定されたことになる。その後、ホストシステム２はこの磁気ディスク装置１に対してアクセスを行い、ハードディスクコントローラ１１、リードライト回路１２及び磁気ヘッド１４等を介して磁気ディスク５０に対するデータの読み出し書き込みを行う。

【００１０】この際、マイクロプロセッサ１９は磁気ディスク５０から磁気ヘッド１４によりサーボデータをアンプ１７、Ａ／Ｄ変換器１８経由で読み出して、前記磁気ヘッド１４を目標トラックにシークさせるためのサーボデータを作成し、これをＤ／Ａ変換回路２０、ドライバ回路２１を介してボイスコイルモータ１６にフィードバックすることによって、前記磁気ヘッド１４を目標トラックに位置決めする制御を行う。尚、利用者は磁気ディスク装置１にパスワードを設定したくない場合は、上記のようなパスワード設定を行わず、通常の磁気ディスク装置と同様にこの装置に対する使用を開始する。

【００１１】ところで、ホストシステム２から磁気ディスク装置１へデータの転送を行う際には、５１２バイト単位で行われるため、マイクロプロセッサ１９には５１２バイトのデータが転送されてくるが、パスワード情報としてはデータの先頭から１００バイトの情報のみが有効となり、図２に示したようになる。尚、パスワード（１００バイト）の内容が全て０である場合には、一旦E^2 ＰＲＯＭに記憶されたパスワードが消去される。

【００１２】上記のように一度パスワードを設定した磁気ディスク装置の電源をオフした後、再度電源をオンとして、この磁気ディスク装置１を使用する場合には、図２のフローチャートに示したような動作が行われる。即ち、電源がオンとなると、ハードディスク装置１のマイクロプロセッサ１９はステップ２０１にて各部の初期設定を行うが、この時、E^2 ＰＲＯＭ２３にパスワードが設定されていることを示す情報があるかないかをステップ２０２にて判定し、パスワードが設定されている場合はステップ２０３へ進み、設定されていない場合はステップ２０６へ飛ぶ。マイクロプロセッサ１９はステップ２０３へ進んだ場合、パスワード確認コマンド入力待ちとなり、ステップ２０４にてホストシステム２からパスワード照合コマンドの実行がなされて、パスワードがホストシステム２から送られてきたか否かを判定する。

【００１３】マイクロプロセッサ１９はステップ２０４にてパスワード照合コマンドでなく、磁気ディスク装置１へのアクセスコマンドがホストシステム２から発行された場合には、このコマンドの実行を行わないで、ステップ２０３に戻る。しかし、パスワード照合コマンドが実行されてパスワードデータが転送されてきた場合にはステップ２０５へ進んで、転送されてきたパスワードがE^2 ＰＲＯＭ２３内に設定されているパスワードと一致するか否かを判定し、一致しない場合はステップ２０３へ戻り、一致した場合はステップ２０６へ進む。ステップ２０６にて、マイクロプロセッサ１９はホストシステム２から発行されるアクセスコマンド入力待ちとなり、その後入力されるアクセスコマンドに対応する処理を行う。一方、ステップ２０２にてパスワードが設定されていない場合、マイクロプロセッサ１９は直ちにステップ２０６へ飛んで、アクセスコマンド入力待ちを行い、本磁気ディスク装置１へのアクセスコマンドの実行を許可した状態になる。

5　　6

【００１４】本実施例によれば、磁気ディスク装置１にパスワードを一旦設定しておけば、この磁気ディスク装置１が何らかの経過で別のホストシステムに接続されても、このホストシステムから前記設定されたパスワードと同一のパスワードが入力されない限り、前記ホストシステムからの磁気ディスク５０へのアクセスを受け付けないため、磁気ディスク５０の記録データが無闇に読み出されることがなくなるため、記録データの盗用を防止することができる。しかも、本例の磁気ディスク装置はＰＣＭＣＩＡインタフェースを備えたホストシステムには着脱自在であり、この点の利便性を確保しつつ、上記した記録データの盗用防止を実現することができる。尚、本発明は据え置き型の磁気ディスク装置にも同様に適用して記録データの盗難防止を図ることができる。

【００１５】

【発明の効果】以上記述した如く本発明の磁気ディスク装置及び記録データ盗用防止方法によれば、接続したホストシステムからのアクセスを簡単に行えないようにして、記録データの盗用を防止することができる。

【図面の簡単な説明】

【図１】本発明の磁気ディスク装置の一実施例を示した＊ブロック図。

【図２】図１に示した磁気ディスク装置の動作開始時の動作を示したフローチャート。

【図３】図１に示した磁気ディスク装置に設定されるパスワート例を示した図。

【符号の説明】

１…磁気ディスク装置　　２…ホストシステム

１１…ハードディスクコントローラ　　１２…リードライト回路

１３…スピンドル　　１４…磁気ヘッド

１５…キャリッジ　　１６…ボイスコイルモータ

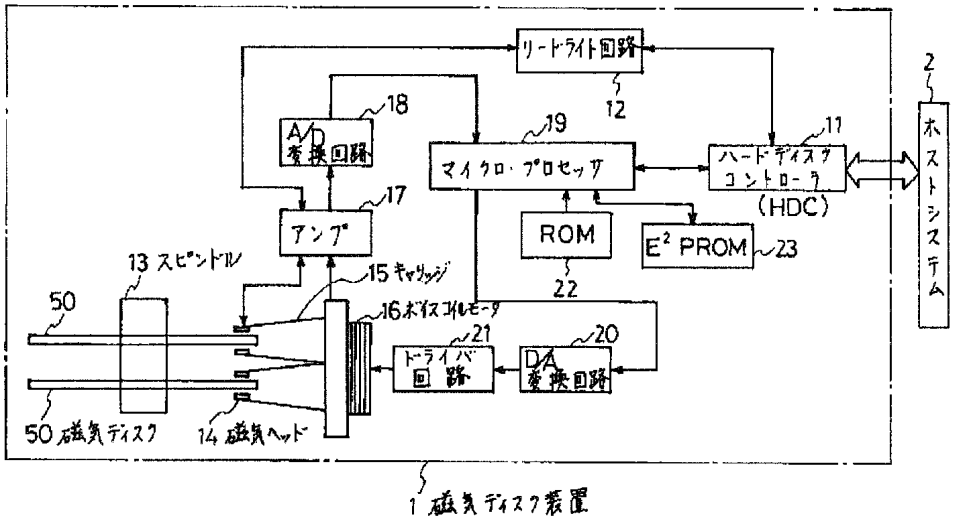
１７…アンプ　　１８…Ａ／Ｄ変換回路

１９…マイクロプロセッサ　　２０…Ｄ／Ａ変換回路

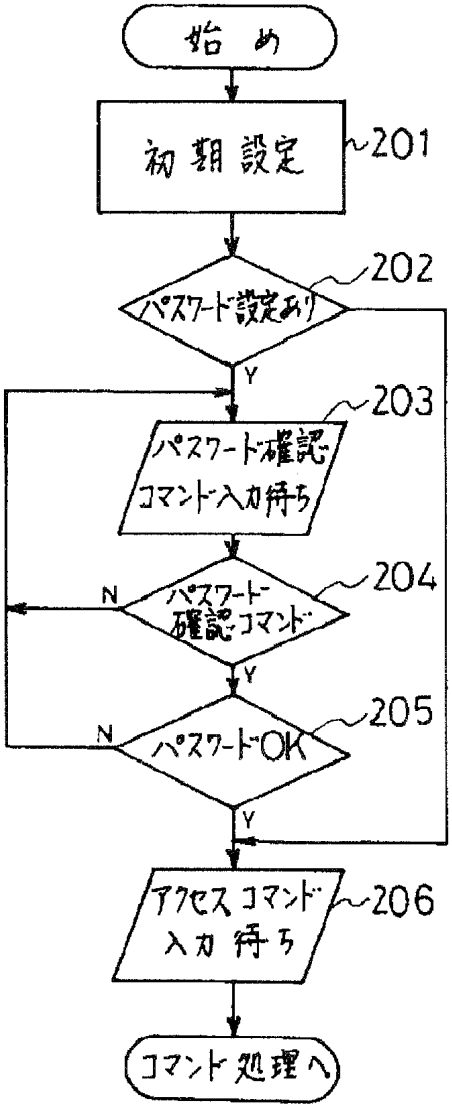
２１…ドライバ回路　　２２…ＲＯＭ

２３…E^2 ＰＲＯＭ　　５０…磁気ディスク

【図１】



【図２】


始め
初期設定
201
パスワード設定あり
202
Y
パスワード確認コマンド入力待ち
203
パスワード確認コマンド
204
N
Y
パスワードOK
205
N
Y
アクセスコマンド入力待ち
206
コマンド処理へ

【図３】

```
0000:    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0010:    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0020:    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0030:    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0040:    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0050:    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0060:    00 01 02 03 00 00 00 00 00 00 00 00 00 00 00 00
0070:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00B0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00E0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00F0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0150:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0160:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0170:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0190:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01A0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01B0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01C0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01D0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01E0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01F0:    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

0000Hから0063H(100バイト)がパスワードデータ

CLAIMS

[Claim(s)]

[Claim 1]A magnetic disk drive which write data to a magnetic disk with an access command from a connected host system, comprising:

Nonvolatile memory which can be written in.

A setting-out means to memorize and set identification information inputted from said host system as said nonvolatile memory.

A control means which performs control which does not execute an access command to said magnetic disk inputted from said host system unless the identification information same at the time of power supply starting as identification information set as said nonvolatile memory is inputted from said host system.

[Claim 2]It is in a surreptitious use prevention method of data currently recorded on said magnetic disk of a magnetic disk drive which write data to a magnetic disk with an access command from a connected host system, At the time of a power turn after setting up identification information inputted from said host system. A record data surreptitious use prevention method not executing an access command to said magnetic disk inputted from said host system unless the same identification information as said set-up identification information is inputted from said host system.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention relates to the method of preventing the theft of the data which was applied to the magnetic disk drive, especially was recorded.
[0002]
[Description of the Prior Art]In recent years, the magnetic disk drive is used with various information processing systems including a personal computer. As a connection method of a magnetic disk drive and a host system, the method which builds a magnetic disk drive in the main part of a host system, and the method which connects a magnetic disk drive to a host system using a connecting cable are common. By the way, in the standard of a PCMCIA interface etc., the portion called a card slot to a notebook type personal computer etc. was provided, and the use of inserting in this portion and using external peripheral equipment, such as a magnetic disk drive, has appeared.
[0003]Since the difference of the magnetic disk drive with such a PCMCIA interface is directly carried out to the slot of a host system and it can be used for it, it is free and simple for the attachment and detachment to a host system. However, as for the path of the magnetic recording medium of a magnetic disk drive which is based on the standard of a PCMCIA interface, 1.8 inches or less are common, Since the size is also miniaturized, suiting a theft easily is expected rather than the connection type which used the conventional inclusion method and cable to the host system. As a measure to the theft of such a small magnetic disk drive, the host system has memorized the password (identification information) and there is a method of not operating, if a right

password is not entered from a user immediately after switching on a power supply. However, in this method, if only the user knows said password, whatever the connected magnetic disk drive, that record data can be read and it turns out that prevention from surreptitious use of the record data of a magnetic disk drive is not effective. Since as for this the conventional magnetic disk drive is made to the last on the assumption that deferment, It is because the method of barring access to the information memorized once it is connected to a host system does not exist in the magnetic disk drive itself, and there was a possibility that record data may be used by stealth.

[0004]

[Problem(s) to be Solved by the Invention]Since the small magnetic disk drive with a PCMCIA interface is [that the attachment and detachment to a host system are easy, and] free, encountering a theft easily is expected. Since the method of barring access to the data which will be recorded if the magnetic disk drive which encountered the theft is connected to the same host system did not exist in the magnetic disk drive itself, there was a danger that record data will be easily used by stealth.

[0005]Then, as this invention removes the above-mentioned fault and cannot perform access from the connected host system easily, an object of this invention is to provide the magnetic disk drive which can prevent surreptitious use of record data, and a record data surreptitious use prevention method.

[0006]

[Means for Solving the Problem]In a magnetic disk drive which write data to a magnetic disk with an access command from a host system to which this invention was connected, Nonvolatile memory which can be written in, and a setting-out means to memorize and set identification information inputted from said host system as said nonvolatile memory, Unless the identification information same at the time of power supply starting as identification information set as said nonvolatile memory is inputted from said host system, it has the composition possessing a control means which performs control which does not execute an access command to said magnetic disk inputted from said host system.

[0007]

[Function]In the magnetic disk drive of this invention, a setting-out means is memorized and set as the nonvolatile memory which can write in the identification information inputted from a host system. A control means performs control which does not execute the access command to said magnetic disk inputted from said host system, unless the identification information same at the time of power supply starting

as the identification information set as said nonvolatile memory is inputted from said host system. Even if a magnetic disk drive is stolen and it is connected to another host system by this, unless the user who uses this host system knows said identification information, the record data of this magnetic disk drive cannot be read, but surreptitious use of record data can be prevented.

[0008]

[Example]Hereafter, one example of this invention is described with reference to drawings. Drawing 1 is a block diagram showing one example of the magnetic disk drive of this invention. It is a host system which 1 passes a magnetic disk drive, and 2 passes a PCMCIA interface for said magnetic disk drive, and connects enabling free attachment and detachment. As opposed to the hard disk controller 11 by which the magnetic disk drive 1 performs reading-and-writing control of data, etc., and the magnetic head 14. Data. The read/write circuit 12 and the magnetic disk 50 which carry out read/write. To the spindle 13 and the magnetic disk 50 to rotate, data. The voice coil motor 16 which drives the magnetic head 14 to write, the carriage 15 made to move the magnetic head 14 to the radial direction of the magnetic disk 50, and the carriage 15, the amplifier 17 which amplifies the servo data read by the magnetic head 14, and servo data. The microprocessor 19 which performs control of the whole A/D conversion circuit 18 and device which are changed into digital data, seek control of the magnetic head 14, etc., D/A converter 19 which changes servo data into analog data, and the voice coil motor 16. It has E^2PROM23 which memorizes ROM22 which stores the various programs which control the driver circuit 21 to drive and the microprocessor 18, and various data, a password, etc. and which is the nonvolatile memory which can be written in.

[0009]Next, operation of this example is explained. When using the magnetic disk drive 1 shown in drawing 1 for the first time and the password is not set up in this device, a user performs operation of setting up the above-mentioned password information, from the keyboard of the host system 2, etc., after equipping the host system 2 with this magnetic disk drive 1. Thereby, the host system 2 sends a password setting command to the magnetic disk drive 1. The microprocessor 19 of the magnetic disk drive 1 will serve as transmission waiting of a password, if a password setting command is received via the hard disk controller 11. On the other hand, a user enters a password as shown in drawing 3 into the host system 2, and makes this password transmit to the microprocessor 19 via the hard disk controller 11. If a password is transmitted, after the microprocessor 19 writes this password in E^2PROM23, it will write in the information which shows that it is in the state where the password is set

up on the E^2PROM23, and will end processing. It means that the password was set up in the magnetic disk drive 1 by this. Then, the host system 2 is accessed to this magnetic disk drive 1, and the read-out writing of data to the magnetic disk 50 is performed via the hard disk controller 11, the read/write circuit 12, and magnetic head 14 grade.

[0010]Under the present circumstances, the microprocessor 19 reads servo data from the magnetic disk 50 by amplifier 17 and A/D-converter 18 course by the magnetic head 14, Control which positions said magnetic head 14 to a target track is performed by creating the servo data for making a target track seek said magnetic head 14, and feeding this back to the voice coil motor 16 via the D/A conversion circuit 20 and the driver circuit 21. A user does not perform the above password setting out but starts the use to this device like the usual magnetic disk drive to set a password as the magnetic disk drive 1.

[0011]By the way, when performing a data transfer from the host system 2 to the magnetic disk drive 1, since it is carried out per 512 bytes, 512 bytes of data is transmitted to the microprocessor 19, but. As password information, only 100 bytes of information become effective from the head of data, and it came to be shown in drawing 2. When all the contents of the password (100 bytes) are 0, the password once memorized by E^2PROM is eliminated.

[0012]When using this magnetic disk drive 1 by considering a power supply as one again after turning off the power supply of the magnetic disk drive which set up the password once as mentioned above, operation as shown in the flow chart of drawing 2 is performed. Namely, if a power supply serves as one, the microprocessor 19 of the hard disk drive 1 will perform initial setting of each part at Step 201, but. At this time, when it judges at Step 202 whether there is any information which shows that the password is set as E^2PROM23, or there is nothing and the password is set up in it, it progresses to Step 203, and when not set up, it flies to Step 206. The microprocessor 19 judges whether it became the waiting for password confirmation command input, execution of the password examination command was made from the host system 2 at Step 204, and the password has been sent from the host system 2, when it progresses to Step 203.

[0013]The microprocessor 19 returns to Step 203 without executing this command, when not a password examination command but the access command to the magnetic disk drive 1 is published from the host system 2 at Step 204. However, when a password examination command is executed and pass word data have been transmitted, it progresses to Step 205, It judges whether the transmitted password is

in agreement with the password set up in E^2PROM23, when not in agreement, it returns to Step 203, and when in agreement, it progresses to Step 206. Processing corresponding to the access command which the microprocessor 19 serves as access command input waiting published from the host system 2, and is inputted after that at Step 206 is performed. On the other hand, when the password is not set up at Step 202, the microprocessor 19 flies to Step 206 promptly, and performs access command input waiting, and execution of the access command to this magnetic disk drive 1 will be permitted it.

[0014]Once it sets the password as the magnetic disk drive 1 according to this example, Even if this magnetic disk drive 1 is connected to another host system by a certain progress, Unless the same password as said set-up password is entered from this host system, in order not to receive access to the magnetic disk 50 from said host system, Since it is lost that the record data of the magnetic disk 50 is read recklessly, surreptitious use of record data can be prevented. And the prevention from surreptitious use of the above-mentioned record data is realizable, being able to detach and attach the magnetic disk drive of this example freely to the host system provided with the PCMCIA interface, and securing the convenience of this point. This invention can be applied also like a non-portable magnetic disk drive, and can aim at theft prevention of record data.

[0015]

[Effect of the Invention]As described above, according to the magnetic disk drive of this invention, and the record data surreptitious use prevention method, as access from the connected host system cannot be performed easily, surreptitious use of record data can be prevented.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The block diagram showing one example of the magnetic disk drive of this invention.
[Drawing 2]The flow chart which showed the operation at the time of the operation start of the magnetic disk drive shown in drawing 1.
[Drawing 3]The figure showing the example of path WATO set as the magnetic disk drive shown in drawing 1.
[Description of Notations]
1 -- Magnetic disk drive 2 -- Host system
11 -- Hard disk controller 12 -- Read/write circuit
13 -- Spindle 14 -- Magnetic head
15 -- Carriage 16 -- Voice coil motor
17 -- Amplifier 18 -- A/D conversion circuit
19 -- Microprocessor 20 -- D/A conversion circuit
21 -- Driver circuit 22 -- ROM
23 -- E^2PROM 50 -- Magnetic disk

[Translation done.]